CAMBRIDGESHIRE
& PETERBOROUGH
COMBINED AUTHORITY

DATA PROTECTION POLICY

Type of document:	Policy
Document produced by:	Cambridgeshire & Peterborough CA Data Protection Officer
Document approved by:	Cambridgeshire & Peterborough Combined Authority Board
Version :	Version 2
Issue date:	
How is this shared?	Email
Date due for review:	Annually April
Reviewer:	Sue Hall

Data Protection Contact		
Contact Details	**Email**	**Phone**
Sue Hall	dpo@cambridgeshirepeterborough-ca.gov.uk	07706 341719

CONTENTS

“If you only read this page then….”

Do ask for only the information you need to do the job and only keep it for as long as you need to

Do be clear about why you are collecting the data

Do only use information for the reason it was collected and seek advice if you need to use it for something else

Do dispose of paper records and emails securely

Do use strong passwords to protect devices and data

Do use secure and encrypted devices

Do make sure you know who you are talking to and check their identity if you need to

Do check someone’s email or postal address before you send anything and make sure you always update records to make sure they are accurate

Do check what is in an envelope or email before you send

Do use the report if any data is lost/misplace/misused, for advice or if someone asks to see information held about them or wants their information deleted

Don’t share personal information unless you are sure you can and you know who is asking

Don’t assume that someone’s consent last forever and covers everything

Don’t leave PCs, laptops and phones unlocked or share your passwords

Don’t leave personal information on show on desks or in vehicles - make sure it's secure

Don’t open emails or click on links if you don’t recognise the sender - speak to IT

Don’t write comments about an individual that we cannot defend - they have a right to see them

Don’t ignore a possible data breach - the sooner it is reported, the sooner it can be dealt with

Don’t think data protection does not matter, it does!

Introduction

We need to collect and use different types of information about people that we provide services for and communicate with in order to deliver those services. These could include current, past and prospective employees, contractors, and suppliers.

In addition, we may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments for business data.

The UK General Data Protection Regulation and Data Protection Act 2018 are pieces of law which will call ("UK GDPR") and ("DPA 2018") respectively, together, "**data protection legislation"**. These explain the requirements and safeguards which we must be applied to personal data to ensure the rights and freedoms of living individuals are not compromised.

Data protection means when we record and use personal information then we must be open about how the information is used and keep it secure. It applies to how we collect, use, share, keep, delete and destroy personal information we use and decide how we use personal information, we have to ensure we comply with data protection legislation.

This policy applies to all personal data held by or on our behalf. It includes manual/paper records and personal data that is electronically processed by computer systems.

Why do we have a policy?

The purpose of this policy is to make sure that we:

- Comply with the law in respect of the data we hold about people
- Protect our customers, employees and other individuals
- Protect the organisation when a data breach happens
- Follow good practice

We recognise we have a responsibility to make sure we comply with all of our data protection duties. We also have to ensure that all of our employees and suppliers not only understand but comply with data protection legislation.

Who does the policy cover?

This policy applies to anyone accessing or using personal information, including for example: employees, temporary or contract staff, volunteers, work placements, contractors, suppliers, service providers or other partners or agencies.

We have to make sure that anyone delivering a service on our behalf complies with this policy and others to make sure our data is safe.

What are our responsibilities?

There are seven Data Protection Principles with which we must comply with in relation to personal information. In summary these are that personal information will be:-

1. **Processed fairly and lawfully in a transparent way**
2. **Obtained only for one or more specified and lawful purposes and not further processed in a manner incompatible with that purpose**
3. **Adequate, relevant and limited to what is necessary**
4. **Accurate and where necessary, kept up to date**
5. **Not be kept for longer than is necessary**
6. **Protected by appropriate technical and organisational measures**
7. **We are accountable and take responsibility for what we do with personal data**

This means that we will:-

a) make sure that when we ask for information then we are fair to the people whose information we ask for and use,
b) explain why we are asking for the information and what we will do with it,
c) make sure we only ask for the information we need,
d) make sure the information we hold is up to date and accurate,
e) make sure we only keep it for as long as we need to,
f) ensure that we have processes in place to protect the information whether it is on paper or electronic,
g) ensure that we won't send information abroad unless there are the proper safeguards,
h) make sure that people can exercise their data protection rights.

In addition we will also:-

- have someone with specific responsibility for data protection (Data Protection Officer, or DPO),
- make sure all employees know that they are responsible for data protection and know what good practice is,
- train staff to manage and handle information correctly,
- support staff to manage and handle personal information correctly,
- respond to any queries about handling personal information promptly and courteously,
- review how we use personal information to make sure we are always complying,
- ensure staff know when they can share information with others.

Lawful basis for processing

We must have a lawful reason to use personal information and special category data. This will be one of the six legal bases in Article 6 of the UK GDPR for personal information:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For special category data then this will be one of the ten legal bases in Article 9 of the UK GDPR:

(a) **Explicit consent:** the individual has given clear consent for you to process their special category data for a specific purpose.

(b) **Employment, social security and social protection**: if authorised by law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018.

(c) **Vital interests:** the processing is necessary to protect someone’s life.

(d) **Not-for-profit bodies:** who process special category data in connection to the activities of charity, clubs, political parties, churches etc.

(e) **Made public by the data subject**.

(f) **Legal claims or judicial acts** if necessary to establish, exercise or defend legal claims.

(g) **Reasons of substantial public interest** with a basis in law and we have identified one of the 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

(h) **Health or social care** with a basis in law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018.

(i) **Public health** with a basis in law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018.

(j) **Archiving, research and statistics** with a basis in law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018.

We should be able to say which applies. If you are not sure, then you should speak to the Data Protection Officer.

What are your responsibilities?

All of us, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to the personal data that we may handle in the course of our work.

All of us must:

- understand the main points of the Data Protection legislation,
- identify and report any risks their line manager,
- make sure that customers understand their rights,
- identify any breaches or loss of data and report them,
- identify and report any rights requests to the Data Protection Team.

People have rights

Data protection legislation has introduced a set of rights for people. These are explained below and how we meet these.

All requests received should be directed to:

The Data Protection Officer
2nd FloorPathfinder House

St Mary's Street

Huntingdon

Cambs

PE29 3TN

Telephone: 07706 341719

Email: dpo@cambridgeshirepeterborough-ca.gov.uk

The Right to be Informed

This means that people have a right to be told what we are doing with their information. We need to be clear and transparent about what we do because this helps build understanding and trust about what we do.

The way we normally tell people about what we do is in what we call a privacy notice. Our privacy notice is available on our website at the link https://cambridgeshirepeterborough-ca.gov.uk/wp-content/uploads/documents/governance/transparency/codes-ofconduct-and-policies/Data-Protection-Policy.pdf so that people can easily find it.

The Right of Access

If we hold information about a person, then they have a right to see their own information. There are a few exceptions to this rule, such as data held for child protection or crime detection / prevention purposes, but most individuals will be able to have a copy of the data held on them. We may have to redact some of the information if we cannot share something with a person.

The Right of Rectification

If a person believes that any of the information that we hold about them is inaccurate, then they have a right to request that we restrict the processing of that information and to rectify the inaccurate personal information. Please note that if the request is to restrict processing their information, we may have to suspend the services provided. We have to respond with a month.

The Right to Erasure

This is popularly known as the “right to be forgotten”. It means that people can ask us to delete or remove information if there no strong reason for us to keep it.

We don’t have to delete information. The below table indicates when we may agree to delete and when we will not

To delete…	Or not to delete…
We no longer need the information	to exercise the right of freedom of expression and information
We should not have the information	We need to keep it to comply with a legal obligation
Our customer withdraws their consent	We need to keep for public health purposes
Legally we should have deleted it	It is of public interest for scientific/historical research or statistical purposes
Our customers object to what we are doing, and we cannot justify keeping the information	We need to keep it for the defence of legal claims

We always need to listen and understand why someone is asking us to delete. We may have to keep some information, for example it is about safeguarding or health and safety. We should still take into account the customer’s concerns and look what we can do to help reduce any distress or concerns they may have.

The Right to Restrict Processing

A person has the right to block or suppress the use of their information. If someone does ask us to restrict the use of their information, then it means that we can retain the information but not use it any further.

We will need to keep some information to ensure that we maintain the restriction.

The Right to Data Portability

Where we have requested a person’s permission to process their personal information or they have provided us with information for the purposes of entering into a contract with us, then they have a right to receive the personal information you provided to us in a portable format.

The Right to Object

An individual can object to what we are doing with their data where if it is based on:

- our legitimate interests or
- public interest or statutory duty or
- direct marketing or
- purposes of scientific/historical research and statistics.
- if the processing is for the exercise of official authority vested in the Authority

The objection must relate to the person's particular situation.

Rights related to automated decision-making including profiling

A person has the right to not be the subject of a decision if it is based on automated processing and it produces a legal effect or significant effect on them.

The right does not apply where processing is necessary for the performance of a contract, authorised by law (including fraud) or there is explicit consent.

What does 'it' mean?

Personal Information

Personal information is information about a living individual who you can identify directly or indirectly from that information. It may also be possible to identify an individual from that and other information which is in the possession of, or likely to come into our possession. It also includes any expression of opinion about the individual and any indication of our intentions.

It is also important to note that information to identify a living person is not limited to names and full addresses. Mapping point data can also potentially identify a person as can limiting the address to postcode.

Special Categories of Personal Information

Special categories of personal data, formerly known as sensitive personal data, means personal data consisting of information as to -

- the racial or ethnic origin of the data subject,
- his/her political opinions,
- his/her religious beliefs or other beliefs of a similar nature,
- whether he/she is a member of a trade union
- genetics
- biometrics
- his/her physical or mental health or condition,
- his/her sexual life,
- sexual orientation

In addition, we would consider the following to be sensitive:

- the commission or alleged commission by him/her of any offence,
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings,
- credit card/debit card details pertaining to the data subject

Data Controller

The Combined Authority is a data controller and will be responsible for ensuring compliance with data protection legislation. It means, on some occasions, that we determine what data is collected and how it is used.

Where someone acts completely on behalf of the authority then we are still the data controller.

You should refer to the contract for providing a service to understand who the data controller is.

Joint Data Controller

There will be occasions where two or more controllers jointly determine what information is collected and why. This could be with Cambridgeshire County Council or Peterborough City Council for example. We need to make sure that customers understand when this is the case.

You should refer to the contract for providing a service to understand when joint controllers exist.

Data Processor

A data processor is the person/service who use the information as per the controller's instructions. A data processor does not own the data and cannot use it for purposes other than stated in the contract or where permitted. Any use or sharing of data should not be done without the written consent of the data controller.

You should refer to the contract for providing a service to understand who the data processor is.

Data Controller-Data Processor Relationship - Contracts

Where the controller and processor are not the same ie the Combined Authority and Cambridgeshire County Council, the relationship must be underpinned by a contract.

It is very important that we have a contract in place for us to deliver services or for something to be done our behalf. The contract has a really important role to play because it makes sure that all concerned understand what should be delivered.

Any contract must contain detailed schedules of the data to be processed as well as the clauses regarding the arrangements for the use, storage, retention and deletion of data by that external party. In all cases, Legal Services will review every contract and ensure that it meets requirements. The contract between the authority and suppliers will make clear that the liabilities and duties of data protection legislation which must be complied with

This kind of terms will be defined in the contract.

Advice on the process for buying and providing services can be obtained from the Data Protection Officer.

When data is lost or goes missing…

We hold information which can be personal and sensitive information but also, for example, commercially sensitive information or simply data.

We must take every care to avoid a data breach by protecting personal information but also by taking steps to avoid losing any data.

In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. You should refer to our data incident reporting policy which covers the process and complete the data incident reporting form.

You must report any breaches, suspected or confirmed, to the Data Protection Officer.

Keeping Information

We may have to keep information, but it must only be kept for as long as we need to.

We will store personal information securely in our IT systems or in hard copy in line with our retention schedule.

We will destroy hard copy personal information securely by using confidential waste bins and electronic records via IT.

More can be found in our Retention Policy.

Location of our information

It is important that we understand where our information is. This does not mean just it's on our devices or on the authority's network. We have to think about where that information really is and the same applies to any data we share or provide to others. This means where servers are or where a cloud/data centre is.

When the UK left the EU, this meant that transfers of information needed to be *permitted* under the UK GDPR. There are provisions in the UK GDPR to enable this flow of information. In order for information to flow from EEA countries, UK needed to be provided with an *adequacy decision* by the EU which it currently has. The UK has also recognised the EU adequacy decisions for non-EEA countries - Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland., and Uruguay.

If the information is being transferred to a country where there is no adequacy decision, such as USA, then we must ensure that we have appropriate safeguards in place. If this is the case, then you should speak to the Data Protection Officer and Legal.

How we handle information

Whenever we handle information then we should do so securely. This should mean that information we store is securely in systems protected by usernames and passwords or filing cabinets that are locked. It also means making sure that only people who should see that information have access. When we share or send information then we should make sure that it is secure.

The sharing of personal information must be by secure means such as secure email or secure file sharing may also be used after review by IT and in line with our IT policy. Failure to comply with this policy will result in the appropriate action being taken under either the relevant policy or contract.

The Sharing of Personal Information

We will only share personal information where a legal gateway exists, or consent has been obtained. Sharing means telling someone some information about them or another person and sharing means giving a supplier a list of people.

You should make sure you know whether you should share personal information and consult the Data Protection Officer if you are not sure.

Disclosures permitted by law

There will be occasions where the disclosure of personal information will be permitted in law such as for the prevention and detection of crime or safeguarding of vulnerable individuals. We will always seek a written request confirming the reason for the disclosure where consent has not been obtained and will evaluate that request before responding. Equally we need to make our own requests in a lawful and proper way.

Information sharing agreements

Any sharing of personal information between organisations may be best supported by an agreement that makes clear what is being shared, why and how. It helps us ensure we are complying with data protection legislation.

Further guidance on the completion of Information Sharing Agreements can be obtained from the Legal department of the Combined Authority.

Testing of systems

We may need to test that computer systems are developed to bring greater efficiency, benefits, and security work appropriately. In order to do so then we will need to consider using personal data in that testing. The first consideration will always be whether personal data is required for testing and the default will be that it is not with anonymised or randomly generated data being used. However, this may not fully test the functionality of a system, therefore consideration must be given to the use of a data snapshot from the live or current system.

We will undertake a data protection impact assessment prior to the use of any current or identifiable data to ensure that this is appropriate and that the appropriate safeguards are in place prior to the export, import and testing. The data will only be held in the test system for the period of testing and then removed. If the testing of the system is being undertaken by a partner or a processor then the same process will apply.

Privacy and the value of information

Data protection is all about privacy. When we use information about people then we have an impact on their privacy in some way.

This could be when we think about buying a new IT system or running a new project or service. It means we need to think about the impact on our customers; how will it affect them? Will it make a change on their lives? Are there any risks that we need to think about? The changes in data protection in 2018 made it mandatory that we have to consider the impact and show that we have. Please refer to the Data Protection Impact Guidance for further information.

Data Protection Impact Assessments (DPIA)

There are two levels of a DPIA; the screening process to work out whether you do need to do a DPIA is the starting point. This should always be completed whenever there are projects, new or changed service activities, or new ICT that could potentially impact on the privacy of individuals.

The completed screening checklist should be shared with the Data Protection Officer to determine whether any further assessment is required. They will inform you as to whether a DPIA is needed.

These can be published so it is important to make sure we have assessed impact and risk.

Only use what you need to use

It can be helpful to think about what level of information you need to use. Do you need to use every bit of information we hold about a person? Can you limit what you do use? You may only need ages and post code for example rather than their name, address, date of birth, NI number, health details and ethnicity.

There are other ways of using personal information without sharing who that person is.

Anonymisation of data

Data can be anonymised ie removal of information which could lead to the identification of an individual. It should be almost statistical because there should be no way that you can identify any individual person. It is not enough to remove the name and address. You should approach the Data Protection Officer for more detailed guidance.

Pseudonymisation

Where it is not necessary to share personal data but anonymised is not sufficient, then consideration should be given to the pseudonymising approach. This means when information is supplied it is not identifiable to the user but the individual producing the information has a “key” to identify.

Information as an asset

When information is organised, stored, used, and analysed then it is an asset that we can use. This means that we need to make sure it is managed properly. This management means that we know what we hold, where it is held, how long for and its qualities. This will help us use the information we have much more efficiently and better because we will understand it more.

Each service will have an Information Asset Owner (IAO) who is responsible for understanding that information, making sure it is only disclosed appropriately and is securely held.

Roles

Chief Executive

The Chief Executive has overall accountability and responsibility for data protection. The Chief Executive is required to provide assurance that all risks relating to data protection and information security are effectively managed and mitigated.

The Chief Executive has delegated responsibility for compliance with the Data Protection Act (including the implementation of this policy and other related policies) to Senior Information Risk Owner.

Senior Information Risk Owner (SIRO)

The named SIRO is responsible for:

- leading and fostering a culture that values, protects, and uses information for the success of the organisation and benefit of its customers,
- overall ownership of the Information Governance policies,
- act as the champion for Information Governance and provide written advice to the on the status of matters within the authority,
- owning the organisation’s overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs,

- advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls,
- owning the organisation’s information incident management framework, and
- ensuring that they receive appropriate training to fulfil the SIRO role.

Data Protection Officer

The Data Protection Officer will:

- manage the compliance with data protection legislation and FOIA,
- maintain an awareness of all IG/IM issues within the authority,
- review and update policies in line with local and national and best practice requirements,
- review and audit all processes and procedures where appropriate and on an ad-hoc basis,
- ensure all line managers and staff are aware of the requirements of these policies and guides,
- set a list of minimum expectations for security standards for IT systems.

Information Risk Group

The authority has a group chaired by the SIRO and attended by representatives of all departments. This is a key group to determining strategy and having oversight of all things data protection.

Responsibilities of Managers

All managers are required to ensure that they and their staff understand this policy and any associated procedures. They are responsible for ensuring that staff are informed and updated on any changes made to this policy.

All managers must identify and report any risks or breaches to the Data Protection Officer.

All line managers must ensure that their staff undertake data protection training and refresher training which will be undertaken annually.

Additional responsibilities for Managers - Temporary Staff

It is a requirement that all temporary staff, agency staff, volunteers, work placement students and all managers requesting access to systems for these temporary workers, should read, and undertake to comply with these compliance guidelines. Managers should ensure that any such staff are trained and understand data protection responsibilities.

Responsibilities of Members

All Members have responsibilities in their own right and when considering the use of personal information for any particular purpose, they should take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful.

Members should also refer to the relevant “Code of Conduct”, which is intended to promote high standards of behaviour amongst the Members of the authority, and which is available on our website.

Responsibilities of all staff

All staff have a responsibility and a duty to abide by the authority’s policies and procedures in handling personal data as well completing any mandatory training provided. They must report any risks or breaches to the Data Protection Officer.

Any breach of this policy or linked to data protection may be considered under the authority’s disciplinary policies.

Policy Review

A review of this policy will take place annually to take account of any new or changed legislation, regulations or business practices.

Monitoring Compliance

Compliance with this policy and related standards and guidance will be monitored and findings will be reported to the Data Protection Officer.

Potential fines for non-compliance with GDPR

The Information Commissioner can issue a monetary penalty for failing to comply with Part 3 of the Act. There are two tiers of penalty higher maximum and the standard maximum.

The higher maximum amount is £17.5million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

Compensation

The GDPR gives an individual the right to claim compensation if damage is suffered as a result of the company breaking data protection law. The ICO cannot award compensation

For further information on compensation, please click on link below:

[Taking your case to court and claiming compensation | ICO]

ICO address

The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, or via their website: https://ico.org.uk/